AMENDMENTS TO THE CLAIMS

Upon entry of this amendment, the following listing of claims will replace all prior versions and listings of claims in the pending application.

IN THE CLAIMS

Please amend claims 1-4, 7-10, 13, 15, 17 and 22 as follows:

1. (Currently Amended) A ~~computer-implemented~~ method of a device for filtering messages routed across a network, the messages including field name-value pairs, the method comprising:

extracting, by a device, field name-value pairs from ~~the~~ messages received via a network;

determining, by the device, ~~for values of the same field name,~~ a most restrictive data type of ~~the~~ values from a plurality of data types of values for a field name of the extracted field name-value pairs; and

storing, by the device, the most restrictive data type in association with the field name.

2. (Currently Amended) The method of claim 1, further comprising:

generating, by the device, a rule which would allow messages having values of a field name that match the most restrictive data type.

3. (Currently Amended) The method of claim 2, further comprising:

applying, by the device, the rule to determine whether to allow messages having values for a field name that match the most restrictive data type.

4. (Currently Amended) The method of claim 1, wherein the determining step further comprises:

determining, by the device, a match factor for a data type, the match factor indicating a fraction of values for the same field name that match the data type; and

selecting, by the device, a data type having a match factor exceeding a threshold and having no child data types with a match factor exceeding the threshold.

5. (Original) The method of claim 4, wherein the threshold is a fraction of values for the same field name which should match the data type.

6. (Canceled).

7. (Currently Amended) A ~~computer-implemented~~ method of a device for filtering Uniform Resource Locator (URL) messages routed across a network, wherein the messages include URL components, the method comprising:

extracting, by a device, URL components from ~~the~~ messages received via a network;

determining, by the device, for URL components at ~~the~~ a same level, with ~~the~~ a same root URL component, a most restrictive data type ~~of the URL component~~ from a plurality of data types of extracted URL components at the same level; and

storing, by the device, the data type in association with the URL components at the same level.

8. (Currently Amended) The method of claim 7, further comprising:

generating, by the device, a rule which would allow messages having the URL components that match the most restrictive data type.

9. (Currently Amended) The method of claim 8, further comprising:

applying, by the device, the rule to determine whether to allow messages having the URL components that match the most restrictive data type.

10. (Currently Amended) The method of claim 7, wherein the determining step further comprises:

determining, by the device, a match factor for a data type, the match factor indicating a fraction of URL components at the same level, with the same root URL component, that match the data type; and

selecting, by the device, a data type having a match factor exceeding a threshold and having no child data types with a match factor exceeding the threshold.

11. (Original) The method of claim 10, wherein the threshold is a fraction of URL components at the same level, with the same root URL component, which should match the data type.

12. (Canceled).

13. (Currently Amended) A ~~computer-implemented~~ method of a device for inferencing a data type of scalar objects from messages routed across a network, the method comprising:

identifying, by a device, scalar objects from messages received via a network, each of the scalar objects having a data type from a plurality of data types;

determining, by the device, a match factor for ~~a~~ each data type of the scalar objects, the match factor indicating a fraction of the scalar objects that match the data type; and

selecting, by the device, a most restrictive data type from the plurality of data types of the scalar objects, the most restrictive data type having a match factor exceeding a threshold and having no child data types with a match factor exceeding the threshold.

14. (Original) The method of claim 13, wherein the threshold is a fraction of scalar objects which should match the data type.

15. (Currently Amended l) A system for inferencing a data type of scalar objects from messages routed across a network, the system comprising:

a module of a device for determining a match factor for ~~a~~ each data type of the scalar objects, the match factor indicating a fraction of scalar objects identified from messages received via a network that match the data type; and

wherein the ~~a~~ module of the device ~~for~~ selects~~ing~~ a most restrictive data type from a plurality of data types of the scalar objects, the most restrictive data type having a match factor exceeding a threshold and having no child data types with a match factor exceeding the threshold.

16. (Canceled).

17. (Currently Amended) A system for filtering messages routed across a network, the messages including field name-value pairs, the system comprising:

a learning engine of a device, for extracting field name-value pairs from ~~the~~ messages received via a network, determining, ~~for values of the same field name~~, a most restrictive data type of ~~the~~ values from a plurality of data types of values for a field name from the extracted field name-value pairs, and storing the most restrictive data type in association with the field name; and

a message filter of the device, for generating a rule which would allow messages having values of a field name that match the most restrictive data type.

18. (Original) The system of claim 17, wherein the learning engine is further adapted to generate a rule which would allow messages having values of a field name that match the most restrictive data type.

19. (Original) The system of claim 17, wherein the message filter is further adapted to apply the rule to determine whether to allow messages having values for a field name that match the most restrictive data type.

20. (Original) The system of claim 17, wherein the learning engine is further adapted to:

determine a match factor for a data type, the match factor indicating a fraction of values for the same field name that match the data type; and

select a data type having a match factor exceeding a threshold and having no child data types with a match factor exceeding the threshold.

21. (Original) The system of claim 20, wherein the threshold is a fraction of values for the same field name which should match the data type.

22. (Currently Amended) A system for filtering Uniform Resource Locator (URL) messages routed across a network, wherein the messages include URL components, the system comprising:

a learning engine of a device, for extracting URL components from ~~the~~ messages received from a network, determining, for URL components at ~~the~~ a same level, with ~~the~~ a same root URL component, a most restrictive data type ~~of the URL component~~ from a plurality of data types of URL components at the same level, and storing the most restrictive data type in association with the URL components at the same level; and

a message filter of the device, for generating a rule which would allow messages having the URL components that match the most restrictive data type.

23. (Original) The system of claim 22, wherein the learning engine is further adapted to generate a rule which would allow messages having the URL components that match the most restrictive data type.

24. (Original) The system of claim 22, wherein the message filter is further adapted to apply the rule to determine whether to allow messages having the URL components that match the most restrictive data type.

25. (Original) The system of claim 22, wherein the learning engine is further adapted to:

determine a match factor for a data type, the match factor indicating a fraction of URL components at the same level, with the same root URL component, that match the data type; and

select a data type having a match factor exceeding a threshold and having no child data types with a match factor exceeding the threshold.

26. (Original) The system of claim 25, wherein the threshold is a fraction of URL components at the same level, with the same root URL component, which should match the data type.